UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/691,170	10/22/2003	Brant L. Candelore	80398P558D	6531

8791 7590 03/16/2007

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025-1030

EXAMINER	
NGUYEN, KHOI	
ART UNIT	**PAPER NUMBER**
2132	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	03/16/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/691,170	CANDELORE, BRANT L.	
	Examiner	Art Unit	
	Khoi Nguyen	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 February 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-32* is/are pending in the application.

4a) Of the above claim(s) *9-22 and 28-31* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-8,23-27 and 32* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *See Continuation Sheet*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Continuation of Attachment(s) 3). Information Disclosure Statement(s) (PTO/SB/08), Paper No(s)/Mail Date :3/25/04, 3/29/04, 01/03/05, 07/21/06, 12/11/06 02/28/07.

DETAILED ACTION

1. Claims 1-8, 23-27, and 32 have been examined.

Election/Restrictions

2. Applicant's election without traverse of Group I-A: Figure 7A, consisting of claims 1-8, 23-27, and 32 in the reply filed on 3/20/2007 is acknowledged.

Priority

3. Applicant's claim for the benefit of a divisional US Application No. 10/388,002 filed March 12, 2003, which claims the benefit of priority of US Provisional Application No. 60/424,381 filed on November 5, 2002 is acknowledged.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1-2, and 7 are rejected under 35 USC 102(e) as anticipated by Pinder et al. (US Pat. No. 6424717), hereafter "Pinder".

Examiner has pointed out particular references contained in the prior arts of record in the body of this action for the convenience of the applicant. Although

the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. Applicant should consider the entire prior art as applicable as to the limitations of the claims. It is respectfully requested from the applicant, in preparing the response, to consider fully the entire references as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the examiner.

6. With regard to claim 1, Pinder discloses a descrambler integrated circuit (IC) adapted to receive scrambled digital content, a message and an encrypted descrambling key (Fig. 2B), comprising

a local memory to store a unique key (Fig. 2B: items 232 and Kpr);

a first process block to decrypt a message using the unique key to produce a key; (Fig. 2B, Items: 234, E_{kpr}(MSK), Kpr, and MSK indicate process block to decrypt a message using unique key to produce a key respectively).

a second process block using the key to decrypt the encrypted descrambling key and to recover a descrambling key (Fig. 2B: item 236, MSK, E_{msk}(CW), CW indicate second process block using the key to decrypt the encrypted descrambling key and to recover the descrambling key respectively).

a descrambler using the descrambling key to descramble the scrambled digital content and to produce digital content in a clear format (Fig. 2B: item 238, CW, E_{cw}(service), Service indicate a descrambler using the descrambling key to

descrambler the scrambled digital content to produce digital content in a clear format respectively).

7. With regard to claim 2, Pinder discloses the descrambler IC (Fig. 2B), wherein the unique key is loaded into the local memory during manufacture of the descrambler IC (col. 11: lines 51-33).

8. With regard to claim 7, Pinder discloses the descrambler IC (Fig. 2B) wherein the first process block and the second process block are logic operating in accordance with one of the following: Data Encryption Standard (DES, Advanced Encryption Standard (AES), and Triple DES (Fig. 3: item 339 and 343).

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. **Claims 3 and 32 is rejected under 35 USC 103(a) as unpatentable over Pinder and in view of Zhang et al (US Pat. No. 6550008), hereafter "Zhang".**

11. With regard to claim 3, Pinder discloses the descrambler IC (Fig. 2B) with the second process block (Fig. 2B: Item 236). However, Pinder does not disclose the descrambler IC, wherein the second process block is a finite state machine. However, Zhang discloses the descrambler IC, wherein the second process block is a finite state machine (col. 5: lines 55-60).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the method of Pinder to include the second process block is a finite state machine, as taught by Zhang to improve protection scheme for broadcast signals or other transmitted information (col. 1: lines 40-43).

12. With regard to claim 32, Pinder's reference has already been discussed. However, Pinder does not discloses a first process block controlled by a non-CPU based state machine to decrypt a message using the unique key to produce a key; a second process block controlled by a non-CPU based state machine using the key to decrypt the encrypted descrambling key and to recover a descrambling key.

However, Zhang discloses a first process block controlled by a non-CPU based state machine (col. 5: lines 57-59) to decrypt a message using the unique key to produce a key; a second process block controlled by a non-CPU based state

machine (col. 5: lines 57-59) using the key to decrypt the encrypted descrambling key and to recover a descrambling key.

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the method of Pinder to include a first process block controlled by a non-CPU based state machine to decrypt a message using the unique key to produce a key, and a second process block controlled by a non-CPU based state machine (col. 5: lines 57-59) using the key to decrypt the encrypted descrambling key and to recover a descrambling key, as taught by Zhang to improve protection scheme for broadcast signals or other transmitted information (col. 1: lines 40-43).

13. Claims 4-6 are rejected under 35 USC 103(a) as unpatentable over Pinder and in view of Ferraro (US Pat. No. 5151782), hereafter "Ferraro".

14. With regard to claim 4, Pinder discloses the descrambler IC (Fig. 2B), wherein the message is a mating key generator (Fig. 2B: item "E_{kpr}(MSK)", "E_{msk}(CW)", and "E_{cw}(Service)", indicate mating key generator(s)).

However, Pinder does not disclose the message is a mating key generator that comprises an identifier of a supplier of the scrambled digital content, the supplier

being one of a cable provider, a satellite-based provider, a terrestrial-based provider, and an Internet service provider.

On the other hand, Ferraro discloses a message comprises an identifier of a supplier of the scrambled digital content, the supplier being one of a cable provider, a satellite-based provider, a terrestrial-based provider, and an Internet service provider (col. 1: Lines 16-23, "HBO" indicates identifier of a supplier of the scrambled digital content).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the method of Pinder to include an identifier of a supplier of the scrambled digital content, the supplier being one of a cable provider, a satellite-based provider, a terrestrial-based provider, and an Internet service provider, as taught by Ferraro to provide more flexible and versatile for switching equipment in the head-end of each cable system of a network of such system (col. 3: lines 4-6).

15. With regard to claim 5, Pinder discloses the descrambler IC (Fig. 2B), with the mating key generator (Fig. 2B: item "E_{kpr}(MSK)", "E_{msk}(CW)", and "E_{cw}(Service)", indicate mating key generator(s)) that enables transmission of the scrambled digital content and the mating key generator message to the descrambler IC (Fig. 3: Item 331, "Transmission Medium", Item 329 "encrypted content", Item 315 "EMM", and Item 333, "Service Reception".

However Pinder does not disclose the descrambler, wherein the mating key generator further comprises an identifier that identifies a provider of a system that enables transmission of the scrambled digital content and the mating key generator message to the descrambler IC.

On the other hand, Ferraro discloses a message further comprises an identifier that identifies a provider of a system that enables transmission of the scrambled digital content and the mating key generator message to the descrambler IC (col. 2: lines 19-22, "an individual cable operator" indicates identifier that identifies a provider of a system that enables transmission of the scrambled digital content and the mating key generator message to the descrambler IC, respectively).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the method of Pinder to include an identifier of a supplier of the scrambled digital content, the supplier being one of a cable provider, a satellite-based provider, a terrestrial-based provider, and an Internet service provider, as taught by Ferraro to provide more flexible and versatile for switching equipment in the head-end of each cable system of a network of such system (col. 3: lines 4-6).

16. With regard to claim 6, Pinder discloses the descrambler IC (Fig. 2B), with the mating key generator (Fig. 2B: item "E_{kpr}(MSK)", "E_{msk}(CW)", and "E_{cw}(Service)",

indicate mating key generator(s)), and a conditional access (CA) system which the scrambled digital content is transmitted (Fig. 1: item 101) and a mating key sequence number (col. 6: lines 25-29).

However, Pinder does not disclose the mating key generator further comprises (i) an identifier that identifies a conditional access (CA) system provider over which the scrambled digital content is transmitted

On the other hand, Ferraro discloses the mating key generator further comprises (i) an identifier that identifies a conditional access (CA) system provider over which the scrambled digital content is transmitted (col. 5: lines 33-35, "Video Cipher II" indicates an identifier that identifies a conditional access (CA) system provider over which the scrambled digital content is transmitted).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the method of Pinder to include an identifier of a supplier of the scrambled digital content, the supplier being one of a cable provider, a satellite-based provider, a terrestrial-based provider, and an Internet service provider, as taught by Ferraro to provide more flexible and versatile for switching equipment in the head-end of each cable system of a network of such system (col. 3: lines 4-6).

17. Claim 8 is rejected under 35 USC 103(a) as unpatentable over Pinder and in view of Alve et al (US Pat. No. 6959090), hereafter "Alve".

18. With regard to claim 8, Pinder disclose the descrambler IC (Fig. 2B) with the unique key (Fig. 2B: items 232 and Kpr). However, Pinder does not disclose the unique key is a one-time programmable value that cannot be read or overwritten once programmed.

Alve, on the other hand, discloses a one-time programmable value that cannot be read or overwritten once programmed (Fig. 4: item 203 and 204).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the method of Pinder to include such that the unique key is a one-time programmable value that cannot be read or overwritten once programmed, as taught by Alve to protect recorded content from illicit reproduction and distribution (col. 1, lines 27-28).

19. **Claim 23 is rejected under 35 USC 103(a) as unpatentable over Pinder in view of Alve, and futher in view of Kocher et al. (US Pat. No. 6640305), hereafter "Kocher".**

20. With regard to claim 23, Pinder discloses a descrambler integrated circuit adapted to receive scrambled digital content and to descramble the scrambled digital content (Fig. 2B), comprising:

a first process block to decrypt a message using a unique key to produce a first key (Fig. 2B, Items: 234, E_{kpr}(MSK), Kpr, and MSK indicate process block to decrypt a message using unique key to produce a key respectively);

a second process block to receive an encrypted second key and, using the first key, to decrypt the encrypted second key in order to recover the second key in a non-encrypted format (Fig. 2B: item 236, MSK, E_{msk}(CW), CW indicate second process block using the key to decrypt the encrypted descrambling key and to recover the descrambling key in a non-encrypted format respectively); and

a descrambler using the second key in the non-encrypted format to descramble the scrambled digital content and to produce digital content in a clear format (Fig. 2B: item 238, CW, E_{cw}(service), CW and Service indicate a descrambler using the descrambling key in the non-encrypted format to descrambler the scrambled digital content to produce digital content in a clear format respectively).

However, Pinder Pinder does not disclose the unique key is a one-time programmable value that cannot be read or overwritten once programmed.

Alve, on the other hand, discloses a one-time programmable value that cannot be read or overwritten once programmed (Fig. 4: item 203 and 204).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify the method of Pinder to include such that the unique key is a one-time programmable value that cannot be read or overwritten once programmed, as taught by Alve to protect recorded content from illicit reproduction and distribution (col. 1, lines 27-28).

Furthermore, neither Pinder nor Alve discloses a first process block to encrypt a message using a unique, one-time programmable key to produce a first key;

Kocher, on the other hand discloses a first process block (Fig. 11: item 1130) to encrypt (Fig. 11: Item "Pseudo-asymetric transform" and 1140) a message using a unique one-time programmable key to produce a first key.

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify methods of Pinder and Alve to include such that the first process block to encrypt a message using a unique, one-time programmable key to produce a first key, as taught by Kocher to distribute content decryption keys in encrypted form to a tamper-resistant cryptographic unit to prevent any attacks (col. 2: lines 45-51).

21. With regard to claim 24, Pinder discloses the descrambler IC (Fig. 2B), wherein the encrypted second key is an encrypted service key (Fig. 2B: Item "E_{msk}(CW)" indicates encrypted service key) associated with at least one selected tier of service (Fig. 22: item 2229, col. 36: lines 56-57, IPPV or NVOD indicates tier of service).

22. With regard to claim 25, Pinder discloses the descrambler IC (Fig. 2B) with the encrypted second key is an encrypted descrambling key (Fig. 2B: Item "E_{msk}(CW)" indicates encrypted service key is an encrypted descrambling key).

However, neither Pinder nor Alve discloses the encrypted second key is an encrypted descrambling key from a smart card in communication with the descrambler IC

Kocher, on the other hand, discloses the encrypted second key is an encrypted descrambling key from a smart card in communication with the descrambler IC (col. 21: lines 47-49).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify methods of Pinder and Alve to include such that the encrypted second key is an encrypted descrambling key from a smart card in communication with the descrambler IC, as taught by Kocher to

distribute content decryption keys in encrypted form to a tamper-resistant cryptographic unit to prevent any attacks (col. 2: lines 45-51).

23. **Claim 26 is rejected under 35 USC 103(a) as unpatentable over Pinder in view of Alve and in view of Kocher and further in view of Ferraro et al. (US Pat No. 5151782), hereafter "Ferraro".**

24. With regard to claim 26, Pinder discloses the descrambler IC (Fig. 2B) where the message decrypted by the first process block is a mating key generator (Fig. 2B: Item MSK indicates a mating key generator).

However, neirther Pinder, Alve, nor Ferraro discloses the message encrypted by the first process block is a mating key generator.

Kocher, on the other hand discloses a first process block (Fig. 11: item 1130) to encrypt (Fig. 11: Item "Pseudo-asymetric transform" and 1140) a message using a unique one-time programmable key to produce a first key.

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify methods of Pinder, Alve, Ferraro and Kocher to include such that the first process block to encrypt a message using a unique, one-time programmable key to produce a first key, as taught by Kocher

to distribute content decryption keys in encrypted form to a tamper-resistant cryptographic unit to prevent any attacks (col. 2: lines 45-51).

Furthermore, neither Pinder, Alve, nor Kocher discloses the message encrypted by the first process block is a mating key generator being a message that comprises an identifier of a manufacturer of a digital device employed with the descrambler IC.

Ferraro, on the other hand discloses the message encrypted by the first process block is a mating key generator being a message that comprises an identifier of a manufacturer of a digital device employed with the descrambler IC (col. 3: lines 45-48).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify methods of Pinder, Alve, Kocher, and Ferraro to include such that the message encrypted by the first process block is a mating key generator being a message that comprises an identifier of a manufacturer of a digital device employed with the descrambler IC, as taught by Ferraro to provide more flexible and versatile for switching equipment in the head-end of each cable system of a network of such system (col. 3: lines 4-6).

25. With regard to claim 27, Pinder discloses the descrambler IC (Fig. 2B) wherein the mating key generator (Fig. 2B: Item MSK indicates a mating key generator) encrypted by the first process block further comprises a service provider identifier, and a conditional access (CA) provider identifier.

However, neirther Pinder, Alve, nor Ferraro discloses the mating key generator encrypted by the first process block further comprises a service provider identifier, and a conditional access (CA) provider identifier.

Kocher, on the other hand discloses a first process block (Fig. 11: item 1130) to encrypt (Fig. 11: Item "Pseudo-asymetric transform" and 1140) a message using a unique one-time programmable key to produce a first key.

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify methods of Pinder, Alve, Ferraro and Kocher to include such that the first process block to encrypt a message using a unique, one-time programmable key to produce a first key, as taught by Kocher to distribute content decryption keys in encrypted form to a tamper-resistant cryptographic unit to prevent any attacks (col. 2: lines 45-51).

Nevertheless, neither Pinder, Alve, nor Kocher discloses the mating key generator encrypted by the first process block further comprises a service provider identifier, and a conditional access (CA) provider identifier

Ferraro, on the other hand discloses the mating key generator encrypted by the first process block further comprises a service provider identifier (col. 2: lines 9-14, "local cable operator" and "delivered by satellite" indicates service provider identifier), and a conditional access (CA) provider identifier (col. 5: lines 33-35, "Video Cipher II" indicates an identifier that identifies a conditional access (CA) system provider over which the scrambled digital content is transmitted).

It would have been obvious to one of the ordinary skill in the art at the time of the applicant's invention was made to modify methods of Pinder, Alve, Kocher, and Ferraro to include such that the mating key generator encrypted by the first process block further comprises a service provider identifier, and a conditional access (CA) provider identifier, as taught by Ferraro to provide more flexible and versatile for switching equipment in the head-end of each cable system of a network of such system (col. 3: lines 4-6).

Conclusion

26. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. US. Pat. No. 5526427 to Thomas et al. (Discloses multi-level encoded signal monitoring system of the Universal Broadcast Code for different data segments from different providers).

b. US. Pat. No. 7146007 to Maruo et al. (Discloses a secure path for digital signaling in an intelligent STB using smartcard).

c. US PGPub No. 2002/0021805 to Schumann et al. (Discloses a content distribution system and method which prevents unauthorized access to secure content using smartcard).

d. US PGPub. 2003/0035540 to Freeman et al. (Discloses decrypting transmissions encrypted by a transmission station having first CA module embedded and second CA module that is removable).

e. US PGPub. 2003/0035543 to Gillon et al. (Discloses index for source of providers and premium level).

f. US PGPub 2003/0059047 to Iwamura (Discloses encrypted video stream from STB, TV, etc. and decrypted in the PC card).

27. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Khoi Nguyen whose telephone number is 570-270-1251. The examiner can normally be reached on Mon-Fri (8:30 am – 5:00 pm est) If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

28. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Khoi Nguyen
Art Unit 2132
Date: 3/14/07

Benjamin E. Lanier
Examiner AU 2132